IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

NATALIE WILLINGHAM individually, and on behalf of all others similarly situated, NADINE HIELSCHER and ROBERT HIELSCHER individually, and on behalf of all others similarly situated, Plaintiffs, v. GLOBAL PAYMENTS, INC., Defendant.	CIVIL ACTION FILE NO. 1:12-CV-01157-RWS-JFK

FINAL REPORT AND RECOMMENDATION

The complaint in this putative class action was filed by Plaintiff Natalie Willingham [Doc. 1] and amended after Global Payments, Inc., filed a motion to dismiss the complaint to add Nadine and Robert Hielscher as Plaintiffs and to cure deficiencies outlined in Defendant's Fed. R. Civ. P. 12(b)(1) and 12(b)(6) motion for dismissal of this action [see Doc. 19]. Plaintiffs' first amended complaint ("FAC") removes a negligence *per se* cause of action; no new causes of action are added. [Doc. 21]. Now pending before the court are Defendant's Rule 12(b)(1) and 12(b)(6) motion

[Doc. 23] to dismiss the FAC, Plaintiffs' response [Doc. 27], and Defendant's reply [Doc. 29].

I. Factual Background

The facts relevant to the court's review of the pending motion are drawn from the FAC and the exhibits attached to Defendant's motion to dismiss. [Doc. 23, Exhibits A-C].[1] Defendant Global Payments, a Georgia corporation in business for over forty years throughout the United States, Canada, Europe, and the Asia-Pacific region, is among other things "a provider of electronic transaction processing services for merchants." [FAC ¶¶ 2, 15, 22]. Defendant "contracts with retailers to handle the processing of card transactions" and, as such, is called a "merchant acquirer" or "credit card processor." [Id. ¶¶ 19, 26]. "[T]he retailer sends consumer information to Global

[1]The court may consider materials attached to a Rule 12(b)(1) motion "if the material is pertinent to the question of the District Court's jurisdiction since it is always the obligation of a federal court to determine if it has jurisdiction." Reeves v. Veterans Admin., 2012 WL 2064505, at *2 (S. D. Ala. May 22, 2012) (citation and internal quotation marks omitted). And, when reviewing a Rule 12(b)(6) motion, the court has discretion to determine whether to accept documents beyond the pleadings, see Adamson v. Poorter, 2007 WL 2900576, at *2 (11th Cir. October 4, 2007) (citations omitted), and may consider documents that are "central" to the complaint and "undisputed." See Atwater v. NFL Players Ass'n, 2007 WL 1020848, at *7 (N.D. Ga. March 29, 2007) (citing Maxcess, Inc. v. Lucent Tech., Inc., 433 F.3d 1337, 1340 n.3 (11th Cir. 2005)).

Payments and Global Payments then forwards that information to Visa, MasterCard, or another issuer, who clears the transaction with the consumer's bank." [Id. ¶ 26].

On March 30, 2012, an internet security website reported: "In separate non-public alerts sent late last week, VISA and MasterCard began warning banks about specific cards that may have been compromised . . . the breached credit card processor was compromised between January 21, 2012[,] and February 25, 2012[,] . . . [and] full Track 1 and Track 2 data was taken -- meaning that the information could be used to counterfeit new cards." [FAC ¶ 28, citing http://krebsonsecurity.com /2012/03/mastercard-visa-warn-of-processor-breach].[2] "Track 1 and Track 2 data refers to the information contained on the magnetic strip located on the back of credit cards. . . . Track 1 typically contains the cardholder's name, account information including account number and expiration data, and other discretionary data. Track 2 . . . does not contain the cardholders' name but only account information, including the account number and expiration date, and other discretionary data." [FAC at 12, n.5 (internal quotation marks omitted)].

[2] The court has included Plaintiffs' citations to websites not for the truth of the matters asserted but because the fact that Plaintiffs allege the website has published such information is central to the complaint and not contested by Defendant. Plaintiffs have not attached a copy of the webpages cited.

Global Payments took the following actions. "By the end of the day on March 30, 2012, Global Payments issued a public statement acknowledging that it had been the target of an attack and had suffered unauthorized third party access into 'a portion of its processing system[ ]'. . . [and] had first learned of the unauthorized access in 'early March of 2012.'" [FAC ¶ 29]. "On April 1, 2012, Global Payments issued a press release indicating the company believed the affected portion of its processing system was confined to North America and that less than 1.5 million card numbers may have been exported." [Id. ¶ 30]. "On April 2, 2012, Global Payments created a website entitled www.2012infosecurityupdate.com [ ] to provide information to consumers . . . [and] repeat[ed] the [ ] information provided . . . in [its] previous public statements." [Id. ¶ 31].

"Also on April 2, 2012, Global Payments held an investor conference call about the unauthorized third party access into Global Payment's computer systems . . . admitted that the breach involved a handful of their servers in their North American system, and . . . indicated that the information exported was believed to be limited to Track 2 data, and so would not include names or social security numbers of consumers." [Id. ¶ 32 (internal quotation marks omitted)]. Global Payments stated that "the 1.5 million potentially affected accounts had not been deactivated *en masse*

and [that] Global Payments would look to the individual issuing institutions to monitor those accounts for fraudulent activity. . . ." [Id.]. "[S]ubsequent reports from Visa and MasterCard indicate the breach could date back to June 7, 2011." [Id. ¶ 34, citing http://krebsonsecurity.com/2012/05/global-payments-breach-window -expands/].

Prior to the announcement of the data breach, Global Payments was listed "as being PCI DSS compliant[,]" that is, it met the "Payment Card Industry Data Security Standard ("PCI DSS")." [FAC ¶¶ 37, 40]. On March 31, 2012, Visa, and, on May 2, 2012, MasterCard removed Global Payments from their lists of PCI DSS compliant payment processors. [Id. ¶ 41]. "In a press release on June 12, 2012, Global Payments continued to . . . indicate the potential card exportation was limited to Track 2 data." [Id. ¶ 35].

After returning home from a trip to Minnesota in mid-March 2012, Plaintiff Natalie Willingham, a resident of Kansas, discovered "fraudulent charges in the approximate amounts of $600 and $300 made to her Bank of America Visa card." [FAC ¶¶ 12, 51, 52]. She alleges, based upon information and belief, that she entered into one or more retail transactions with a merchant who contracts with Global Payments and that Defendant, upon receiving her sensitive "Personally Identifiable Information" ("PII") "owed a duty to [Plaintiff] . . . including the obligation to prevent

that data from being stolen by outside attackers or hackers." [Id. ¶¶ 53, 54]. Willingham alleges that Global Payments breached this duty -- that her "PII was compromised by Defendant through its misconduct [and] continuing failure to provide [Plaintiff] with proper notification of the Data Breach." [Id. ¶ 55].

Plaintiffs Nadine and Robert Hielscher, who reside in California, have a Visa branded debit card issued by Chase Bank. [FAC ¶¶ 13, 14, 58]. "On April 2, 2012, upon access by an unauthorized user, Robert Hielscher's debit card information was used to purchase products from Alliance Sports Group at NEBOtools.com in the amount $349.90. [The Hielschers] obtained a receipt for this transaction, which included Robert Hielscher's name and home address. It also included the name, email address, home address and phone number of a person unknown to [them] in Tampa, Florida." [Id. ¶ 59]. "The following day, April 3, 2012, upon access by an unauthorized user, Robert Hielscher's debit card information was used to purchase products from militarygear.com in the amount of $303.96." [Id. ¶ 60]. Upon information and belief, the Hielschers allege that they "entered into a retail transaction with a merchant who contracts with Global Payments for credit card processing or other services, that Global Payments "obtained [their] sensitive PII [and] owed [them] a duty . . . including the obligation to prevent that data from being stolen by outside

attackers or hackers [and] breached this duty . . . through its misconduct [and] continuing failure to provide [Plaintiffs] with proper notice of the Data Breach." [Id. ¶¶ 61-63].

Plaintiffs' FAC alleges causes of action for: negligence (Count I); violation of the Federal Stored Communications Act ("SCA"), 18 U.S.C. §§ 2702(a)(1), (a)(2), (Count II); willful and negligent violation of the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. § 1681(b), (Counts III and IV); violation of the Georgia Uniform Deceptive Trade Practices Act ("UDTPA"), O.C.G.A. §§ 10-1-372(5), (7), (12), (Count V); and third party beneficiary (Count VI) and implied contract (Count VII) breach of contract claims. Plaintiffs allege that:

> As a direct and proximate cause of Defendant's conduct, Plaintiffs and Class Members *have suffered, and will continue to suffer damages,* including, but not limited to, monetary loss for fraudulent charges; interest, overdraft or "overlimit" penalties on their accounts; fear and apprehension of fraud, abuse, loss of money, and identity theft; actual identity theft; loss of privacy; the burden and cost of monitoring their credit, bank accounts and credit history; the burden and cost of closing compromised accounts and opening new accounts; the burden of closely scrutinizing credit card statements for past and future transactions; loss of time spent seeking to prevent or undo harm by monitoring their bank and credit, damages to their credit history; loss of privacy; anxiety and emotional distress, and other economic and noneconomic damages.

[Id. ¶¶ 97, 113, 125, 170, 183 (emphasis added)].[3] Defendant contends that the FAC still fails to allege sufficient facts to establish Article III standing or to state a claim for which relief can be granted against Defendant.

Additional facts will be set forth as needed in the court's discussion of the Defendant's motion to dismiss the FAC.

II. Rule 12(b)(1) Motion to Dismiss

The court must first address Defendant's Rule 12(b)(1) motion to dismiss Plaintiffs' putative class action for lack of Article III standing. "[P]rior to the certification of a class, and technically speaking before undertaking any formal typicality or commonality review, the district court must determine that at least one named class representative has Article III standing to raise each class subclaim." Prado-Steiman ex. rel. Prado v. Bush, 221 F.3d 1266, 1280 (11th Cir. 2000). "[I]f none of the named plaintiffs purporting to represent a class establishes the requisite of a case or controversy with the defendants, none may seek relief on behalf of himself or any other member of the class." O'Shea v. Littleton, 94 S. Ct. 669, 675 (1974).

[3]Counts IV and V allege similar injuries based on the same factual allegations. See FAC ¶¶ 130, 150.

"'In essence the question of [Article III] standing is whether the litigant is entitled to have the court decide the merits of the dispute or of particular issues.'" Wright v. Dougherty County, Georgia, 358 F.3d 1352, 1355 (11th Cir. 2004) (quoting Warth v. Seldin, 95 S. Ct. 2197, 2205 (1975)). If the litigant cannot demonstrate Article III standing, the court lacks subject matter jurisdiction to review the plaintiff's claims. Article III limits the power of federal courts to the adjudication of actual "cases" and "controversies." U.S. Const. art. III, § 2.

Rule 12(b)(1) Standard of Law

When a defendant challenges the court's subject matter jurisdiction by bringing a Rule 12(b)(1) motion, the plaintiff bears the burden to establish that jurisdiction exists. Lujan v. Defenders of Wildlife, 112 S. Ct. 2130, 2136 (1992). "[T]he district court is free to independently weigh facts, and may proceed as it never could under Rule 12(b)(6). . . . That is, when a Rule 12(b)(1) motion constitutes a factual attack on subject matter jurisdiction no presumptive truthfulness attaches to plaintiff's allegations, and the existence of disputed material facts will not preclude the trial court from evaluating for itself the merits of the jurisdictional issue."[4] Turcios v. Delicias

[4]An attack on subject matter jurisdiction can either be a "facial attack" or a "factual attack." See Scarfo v. Ginsberg, 175 F.3d 957, 960 (11th Cir. 1999). "Facial attacks on a complaint require the court merely to look and see if the plaintiff has

Hispanas Corp., 275 Fed. Appx. 879, 880 (11th Cir. 2008) (quoting Morrison v. Amway Corp., 323 F.3d 920, 925 (11th Cir. 2003)) (internal quotation marks omitted).

The Eleventh Circuit has "cautioned, however, that the district court should only rely on Rule 12(b)(1) [i]f the facts necessary to sustain jurisdiction *do not implicate the merits of plaintiff's cause of action*." Turcios, 275 Fed. Appx. at 880 (citation and internal quotation marks omitted) (emphasis in original). "[J]urisdiction becomes intertwined with the merits of a cause of action when a statute provides the basis for both the subject matter jurisdiction of the federal court and the plaintiff's substantive claim for relief." Id. (citation and internal quotation marks omitted). "If a jurisdictional challenge does implicate the merits of the underlying claim then: [T]he proper course of action for the district court is to find that jurisdiction exists and deal with the objection as a direct attack on the merits of the plaintiff's case[,]" id. (citation and internal quotation marks omitted), because "[j]udicial economy is best promoted when the existence of a federal right is directly reached . . . [,]" Garcia v. Copenhaver,

---

sufficiently alleged a basis of subject matter jurisdiction, and the allegations in [the] complaint are taken as true for the purposes of the motion. . . . Factual attacks challenge the existence of subject matter jurisdiction in fact, irrespective of the pleadings, and matters outside the pleadings, such as testimony and affidavits, are considered." Id. (quoting Lawrence v. Dunbar, 919 F.2d 1525, 1529 (11th Cir. 1990)) (internal quotation marks omitted). Defendant's Rule 12(b)(1) motion is a factual attack on the court's power to hear the case.

Bell & Associates, M.D.'s, P.A., 104 F.3d 1256, 1261 (11th Cir. 1997) (citation and internal quotation marks omitted).

Discussion

To prove constitutional standing under Article III, a plaintiff must show three things:

> First, the plaintiff must have suffered an injury in fact - an invasion of a legally protected interest which is (a) concrete and particularized, and (b) actual or imminent, not conjectural or hypothetical. Second, there must be a causal connection between the injury and the conduct complained of-the injury has to be fairly . . . trace[able] to the challenged action of the defendant, and not . . . th[e] result [of] the independent action of some third party not before the court. Third, it must be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.

Bischoff v. Osceola County, Fla., 222 F.3d 874, 883 (11th Cir. 2000) (quoting Lujan, 112 S. Ct. at 2136) (internal quotation marks omitted). That is, "[t]o establish standing, a plaintiff must present an injury that is concrete, particularized, and actual or imminent; fairly traceable to the defendant's challenged action; and redressable by a favorable ruling." Horne v. Flores, 129 S. Ct. 2579, 2592 (2009); accord Turcios, 275 Fed. Appx. at 880.

The fraudulent charges on Plaintiffs' card accounts are "fairly traceable" to the data theft. A showing that an injury is "fairly traceable" requires less than a showing

of "proximate cause." Resnick v. AvMed, Inc., 693 F.3d 1317, 1324 (11th Cir. 2012) (holding that use of sensitive PII ten and fourteen months after laptop was stolen was sufficient to demonstrate that identity theft was fairly traceable to the theft of the laptop and plaintiffs' sensitive PII); accord Focus on the Family v. Pinellas Suncoast Transit Authority, 344 F.3d 1263, 1273 (11th Cir. 2003) ("fairly traceable" standard does not require proof of causation beyond a reasonable doubt or by clear and convincing evidence). But Defendant argues that Plaintiffs have not sufficiently alleged an injury-in-fact that is either actual or imminent or redressable and that Plaintiffs have not demonstrated that the fraudulent charges on their accounts are fairly traceable to Defendant's actions.

Plaintiffs argue, in response, that the amended complaint alleges "at least three recognizable injuries[:] that their PII was stolen by, and remains in the hands of, hackers[,] . . . that their PII was used by these hackers . . . to [ ] purchase items with Plaintiffs' identities[, and that Defendant] failed . . . to promptly notify Plaintiffs and Class Members of the data breach and . . . so has prevented those affected by the data breach from taking proper preventative measures to protect from further identity theft." [Doc. 27 at 3]. Plaintiffs contend that they have thus demonstrated an actual injury-in-fact. In support, Plaintiffs cite the Eleventh Circuit decision in AvMed, Inc. as having

"recognized that sister circuits have found that even the threat of future identify theft is sufficient to confer standing in similar circumstances." [Doc. 27 at 4, citing AvMed, Inc., 693 F.3d at 1322]. Plaintiffs also cite Irwin v. RBS Worldpay, Inc., Civil Action No. 1:09-cv-00033, Order, Doc. 59 (N.D. Ga. February 5, 2010) (hereinafter cited as "RBSW at --"),[5] contending that RBSW is "a case involving substantially similar allegations to those in this case, [in which] this Court specifically found that claimed damages associated with 'the risk of future identity theft' are recoverable." [Doc. 27 at 4]. As Plaintiffs correctly argue, this Court's decision in RBSW stands for the proposition that "'as long as the plaintiff sufficiently pled that he or she actually suffered identity theft, the court will allow recovery of damages associated with the risk of future identity theft and associated mitigation efforts . . . .'" [Id. at 5 (citation omitted)].[6]

---

[5]A copy of the decision in RBSW is attached to Defendant's motion to dismiss. [Doc. 23, Exhibit A]. Because there were two plaintiffs in RBSW and the court reached a different holding as to each plaintiff, the court will refer to the case by the defendant's name.

[6]It is unclear whether Plaintiffs intend to quote RBSW or the Bell case cited in RBSW. The relevant portion of the Court's Order in RBSW states: "as explained in Bell v. Acxion Corporation, 2006 WL 2850042, at *2 (E.D. Ark. October 3, 2006), *if* the complaint sufficiently alleges that identity theft actually occurred, then the plaintiff's claims of mitigation expenses and the increased risk of identity theft were sufficient as damages." RBSW at 10-11 (emphasis added). In Bell, the court stated:

Defendant contends that Plaintiffs have not sufficiently pled an actual, concrete loss or injury. [See Doc. 23-1 at 7; Doc. 29 at 4]. Defendant argues that Plaintiffs' allegations of fraudulent charges on their cards are like the allegations of the plaintiff Badish in RBSW, as to whom the Court held that there was "no injury-in-fact when bank removed unknown charge on plaintiff's credit card." [Doc. 23-1 at 7]. This Court rejected the "conclusion that [Badish] has been a victim of identity theft simply because she noted a charge from Staples on her bank statement that was unknown to her, but was later removed by the bank." RBSW at 9. To sufficiently allege that identity theft actually occurred, a plaintiff must, thus, allege more than fraudulent charges which were removed.

Plaintiff Willingham alleges only that she discovered "fraudulent charges in the approximate amounts of $600 and $300 made to her Bank of America Visa card." [FAC ¶ 52]. The Court's decision in RBSW regarding Badish indicates that without some further factual allegation, such as that Plaintiff was not reimbursed for those charges or that she incurred fees or other expenses or financial consequences because

---

"[W]hile there have been several lawsuits alleging an increased risk of identity theft, no court has considered the risk itself to be damage. Only where the plaintiff has actually suffered identity theft has the court found that there were damages." Id., 2006 WL 2850042, at *2.

of such charges, Plaintiff Willingham has not sufficiently pled an actual injury-in-fact that establishes Article III standing. Plaintiff Willingham's conclusory allegation that "Plaintiffs and Class Members have suffered, and will continue to suffer damages" [FAC ¶¶ 97, 113, 125, 170, 183] does not suffice to establish Article III standing. Willingham must plead sufficient facts to demonstrate that she has suffered an injury-in-fact and thus has an actual case or controversy to bring before the court. See Key v. DSW, Inc., 454 F. Supp. 2d 684, 687-89 (S.D. Ohio 2006) (plaintiff failed to allege injury-in-fact for Article III standing after unauthorized access to her personal data where plaintiff alleged that the class "incurred the cost and inconvenience of, among other things, canceling credit cards, closing checking accounts, ordering new checks, obtaining credit reports and purchasing identity and/or credit monitoring" but plaintiff's only alleged injury was "hav[ing] been subjected to a substantial increased risk of identity theft or other related financial crimes").

In the absence of actual injury-in-fact, the court must consider whether Plaintiff Willingham has nonetheless pled sufficient facts to demonstrate that the risk of future identity theft and related expenses which she alleges is an "imminent" risk. "Where there is no actual harm, [ ] its *imminence* (though not its precise extent) must be established." Lujan, 112 S. Ct. at 2138 n.2 (emphasis added); accord Reilly v.

Ceridian Corp., 664 F.3d 38, 42 (3rd Cir. 2011) ("'The complainant must allege an injury to himself that is distinct and palpable, as distinguished from merely abstract, and the alleged harm must be actual or imminent, not conjectural or hypothetical.'") (quoting Whitmore v. Arkansas, 110 S. Ct. 1717, 1723 (1990)) (internal quotation marks omitted). The imminence requirement for Article III standing "ensures that courts do not entertain suits based on speculative or hypothetical harms." Pub. Interest Research Group of N.J., Inc. v. Magnesium Elektron, Inc., 123 F.3d 111, 122 (3rd Cir. 1997)

In RBSW, after finding that Badish had not pled an actual injury-in-fact, the Court held that Badish had also not established a risk of imminent future identity theft and associated mitigation efforts. RBSW at 11-12. Plaintiff Willingham's allegations, likewise, do not suffice to establish an imminent risk of future identity theft or mitigation expenses. Plaintiff's alleged increased risk of future identity theft, like the plaintiff's alleged risk of future injury in Reilly, "is dependent on entirely speculative, future actions of an unknown third-party." Id., 664 F3d at 42.[7]

[7]Pisciotta v. Old Nat. Bancorp., 499 F.3d 629 (7th Cir. 2007), cited by Plaintiff [Doc. 27 at 5], is not binding on this court and is not persuasive. Pisciotta "relied on cases . . . which addressed increased risk of future medical injury [or] increased risk of future environmental injury[,]" Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d 1046, 1051 (E.D. Mo. 2009) (citing Pisciotta, 499 F.3d at 634 n.3), the two areas of

With regard to the Hielschers, their factual allegations are more detailed than Willingham's allegations. Plaintiffs allege that "Robert Hielscher's debit card information was used to purchase products from Alliance Sports Group at NEBOtools.com in the amount $349.90 [and] a receipt for this transaction [ ] included Robert Hielscher's name and home address [as well as] the name, email address, home address and phone number of a person . . . in Tampa, Florida[,]" who was unfamiliar to the California couple [and that on the] following day, April 3, 2012, upon access by an unauthorized user, Robert Hielscher's debit card information was used to purchase products from militarygear.com in the amount of $303.96." [FAC ¶¶ 59, 60]. The Hielschers' allegations fall short, however, of the factual allegations by the plaintiff Irwin in RBSW. Irwin alleged that "his credit reports [on two dates] indicated that credit was applied for . . . [and he was] unfamiliar with . . . the . . . credit applications[,]" a public record report indicated that a person unknown to Irwin was using his social security number, and his credit reported listed a previous address unknown to him. RBSW at 8 & n.7. This Court held that Irwin's allegation of identity theft was "adequately supported by multiple factual allegations that are suggestive of

---

harm where several Circuit Courts have held that a risk of future harm is sufficient to establish standing. Accord Bouldry v. C.R. Bard, Inc., -- F. Supp. 2d --, 2012 WL 6599829, at *3 (S.D. Fla. December 18, 2012) (suit for medical monitoring expenses).

identity theft, and thus [his] claim of identity theft sufficiently confers Article III standing." Id. at 9-10. The Hielschers' allegations also fall short of the allegations by the plaintiffs in the AvMed, Inc. case cited by Plaintiffs.

In AvMed, Inc., one plaintiff, Curry, alleged that ten months after a laptop containing her sensitive information was stolen from AvMed, Inc., "Bank of America accounts were opened in [her] name, credit cards were activated, and the cards were used to make unauthorized purchases . . . [her] home address was also changed with the U.S. Postal Service"; another plaintiff, Moore, alleged that his sensitive information was used fourteen months after the laptop theft and "an account was opened in [his] name with E*Trade Financial, and [later] overdrawn." AvMed, Inc., 693 F.3d at 1322. The Eleventh Circuit held that such allegations established both injury-in-fact and causation, as well as a redressable injury. Id. at 1322-24. The Hielschers' allegations that they had fraudulent charges on their account are, in comparison, threadbare, and Defendant argues that Plaintiffs' failure to allege "that they actually paid for the fraudulent charges . . . is no oversight." [Doc. 23-1 at 7].

The failure of all Plaintiffs to plead that they were not reimbursed or that the charges were not removed appears to be a "direct result of plaintiffs' inability to plead or prove" actual identity theft. In re Jetblue Airways Corp. Privacy Litigation, 379 F.

Supp. 2d 299, 326 (E.D. N.Y. 2005) (finding that plaintiffs were unable to plead or prove actual injury). Plaintiffs' PII does not have an inherent monetary value. See In re Facebook Privacy Litig., 2011 WL 6176208, at *5 (N.D. Cal. November 22, 2011). And Plaintiffs have not directed the court's attention to, nor has the court found, any precedent for holding that Plaintiffs' allegations, without further evidence of identity theft, are sufficient to establish either an actual or imminent risk of injury-in-fact for Article III standing. In light of the Eleventh Circuit's cautionary language in Turcios, 275 Fed. Appx. at 880, however, the undersigned recommends that the District Court "decline[ ] to hold at this juncture that, as a matter of law, [Plaintiffs have] failed to [and could not, if allowed leave to amend the complaint a second time] allege an injury in fact sufficient to support Article III standing." Claridge v. RockYou, Inc., 785 F. Supp. 2d 855, 861 (N.D. Ca. 2011).[8]

Defendant's injury-in-fact Article III arguments "subsume" Defendant's Rule12(b)(6) arguments that Plaintiffs cannot state a claim for relief for a compensable injury. RockYou, Inc., 785 F. Supp. 2d at 860. Stated differently, "Defendant[']s]

[8]Had there been no fraudulent charges on Plaintiffs' cards, the court would recommend that Defendant's Rule 12(b)(1) motion be granted, as did the Third Circuit in Reilly, 664 F.3d at 42, and the court (and cases cited) in Hammond v. The Bank of New York Mellon Corp., 2010 WL 2643307, at **1, 2 (S.D. N.Y. June 25, 2010).

arguments are [more] directed at the issues plaintiff[s] wish[ ] to adjudicate, rather than whether plaintiff[s have] alleged a personal stake in the outcome of this action." State Farm Mut. Auto. Ins. Co. v. Mallela, 2002 WL 31946762, at *7 (E.D. N.Y. November 21, 2002). "The question of whether [Plaintiffs'] allegations are sufficient to state a claim under substantive law should be addressed in a motion to dismiss under Rule 12(b)(6), not a challenge to [Plaintiffs'] Article III standing." Id.; accord Turcios, 275 Fed. Appx. at 880. Because the court recommends *infra* that Defendant's Rule 12(b)(6) motion to dismiss be granted as to each cause of action in the FAC, the court **RECOMMENDS** that Defendant's Rule 12(b)(1) motion be **DENIED AS MOOT**.[9]

III. Rule 12(b)(6) Motion to Dismiss

Turning to Global Payment's Fed. R. Civ. P. 12(b)(6) motion, the court will first address the federal claims alleging violation of the SCA and FCRA and then address

[9]The court's recommendation does not prevent Defendant from raising the issue of standing at a later stage should any of the Plaintiffs' claims survive Defendant's Rule 12(b)(6) motion to dismiss the complaint after the District Court's review of this report and recommendation. "As litigation progresses, Article III places an increasingly demanding evidentiary burden on parties that seek to invoke federal jurisdiction." People to End Homelessness, Inc. v. Develco Singles Apartments Associates, 339 F.3d 1, 8 (1st Cir. 2003). And "[a] plaintiff who has standing at the motion to dismiss stage, does not automatically have standing at the summary judgment or trial stage." Id.

Plaintiffs' state law claims for deceptive trade practices in violation of the Georgia UDTPA, negligence, and breach of contract.

Rule 12(b)(6) Standard of Law

On a motion to dismiss under Rule 12(b)(6), the complaint's factual allegations are assumed true and construed in the light most favorable to the plaintiff. Hardy v. Regions Mortg., Inc., 449 F.3d 1357, 1359 (11th Cir. 2006); M.T.V. v. DeKalb County School Dist., 446 F.3d 1153, 1156 (11th Cir. 2006). "However, conclusory allegations, unwarranted deductions of facts or legal conclusions masquerading as facts will not prevent dismissal." Oxford Asset Mgmt., Ltd. v. Jaharis, 297 F.3d 1182, 1188 (11th Cir. 2002) (citations omitted).

The Federal Rules of Civil Procedure include no requirement that a plaintiff detail the facts upon which the plaintiff bases a claim. Rule 8(a)(2) requires a complaint to contain "a short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2) (as amended 2007). And Rule 10(b) provides in pertinent part that "[a] party must state its claims . . . in numbered paragraphs, each limited as far as practicable to a single set of circumstances. . . . If doing so would promote clarity, each claim founded on a separate transaction or

occurrence . . . must be stated in a separate count. . . ." Fed. R. Civ. P. 10(b) (as amended 2007).

"While a complaint . . . does not need detailed factual allegations, . . . a plaintiff's obligation to provide the 'grounds' of his 'entitle[ment] to relief' requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do[.]" Bell Atlantic Corp. v. Twombly, 127 S. Ct. 1955, 1964-65 (2007) (citations omitted); accord Financial Sec. Assurance, Inc. v. Stephens, Inc., 500 F.3d 1276, 1282-83 (11th Cir. 2007) (recognizing that "while notice pleading may not require that the pleader allege a specific fact to cover every element or allege with precision each element of a claim, it is still necessary that a complaint contain either direct or inferential allegations respecting all the material elements necessary to sustain a recovery under some viable legal theory") (citations and internal quotation marks omitted). "Factual allegations must be enough to raise a right to relief above the speculative level . . . , on the assumption that all the allegations in the complaint are true (even if doubtful in fact)[.]" Twombly, 127 S. Ct. at 1965 (citations omitted). "Stated differently, the factual allegations in a complaint must 'possess enough heft' to set forth 'a plausible entitlement to relief[.]'" Stephens, Inc., 500 F.3d at 1282 (quoting Twombly, 127 S. Ct. at 1966-67). A plaintiff's complaint will be dismissed

if it does not contain "factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Ashcroft v. Iqbal, 129 S. Ct. 1937, 1949 (2009) (citation omitted). "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." Id.

The court's inquiry at this stage of the proceedings focuses on whether the challenged pleadings "give the defendant fair notice of what the . . . claim is and the grounds upon which it rests." Erickson v. Pardus, 127 S. Ct. 2197, 2200 (2007) (citations and internal quotation marks omitted). And, a court reviewing a motion to dismiss must keep in mind that a "motion to dismiss for failure to state a claim upon which relief can be granted merely tests the sufficiency of the complaint; it does not decide the merits of the case." Wein v. American Huts, Inc., 313 F. Supp. 2d 1356, 1359 (S.D. Fla. 2004) (citing Milburn v. United States, 734 F.2d 762, 765 (11th Cir. 1984)). "Regardless of the alleged facts, however, a court may dismiss a complaint on a dispositive issue of law." Bernard v. Calejo, 17 F. Supp. 2d 1311, 1314 (S.D. Fla. 1998) (citing Marshall County Bd. of Educ. v. Marshall County Gas Dist., 992 F.2d 1171, 1174 (11th Cir. 1993) ("[T]he court may dismiss a complaint . . . when, on the basis of a dispositive issue of law, no construction of the factual allegations will

support the cause of action.")); see also Glover v. Liggett Group, Inc., 459 F.3d 1304, 1308 (11th Cir. 2006) (same).

The court will apply these standards in ruling on Defendant's motion to dismiss the claims asserted in Plaintiffs' amended complaint.

Rule 12(b)(6) Discussion

A. SCA Claims

Title II of the Electronic Communications Privacy Act ("ECPA") created the SCA[10] in 1986 "for the express purpose of addressing 'access to *stored* . . . electronic communications and transactional records.'" Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878-79 (9th Cir. 2002) (quoting S.Rep. No. 99-541, at 3, 1986 USCCAN 3555, 3557) (emphasis omitted); accord United States v. Steiger, 318 F.3d 1039, 1047 (11th Cir. 2003). Because "'the ECPA was written prior to the advent of the Internet and the World Wide Web[,] . . . Courts have struggled to analyze problems involving modern technology within [its] statutory framework[.]'" Steiger, 318 F.3d at 1047 (quoting Konop, 302 F.3d at 874).

[10]The SCA is the "Stored Wire and Electronic Communications and Transactional Records Access" Act, under Title 18 of the United States Code, Part I (Crimes), Chapter 121, and is also referred to as the "SWECA." See, e.g., Jones v. H Group, Inc., 2012 WL 195724, at *1 (D. Or. January 23, 2012).

The SCA applies to two types of services. Section 2702(a)(1) of the SCA provides that "a person or entity providing an electronic communication service [("ECS")] to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1). Section 2702(a)(2)(A) of the SCA provides that "a person or entity providing a remote computing service [("RCS")] to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service on behalf of . . . a subscriber or customer of such service." 18 U.S.C. § 2702(a)(2)(A).

In Count II of the FAC, Plaintiffs claim that Global Payments is an ECS offering services to the public, that Defendant violated the SCA by "failing to take commercially reasonable steps to safeguard [their] sensitive PII while in electronic storage and by continuing to process payments despite not being PCI DSS compliant" and that such conduct "amounts to knowingly allowing unauthorized access to its processing system and knowingly divulging customer credit and debit account information[,]" in violation of 18 U.S.C. § 2702(a)(1). [FAC ¶¶ 102, 106]. Plaintiffs claim that Defendant is also an RCS offering services to the public and that "[b]y failing to take commercially reasonable steps to safeguard sensitive consumer financial

data and PII, including [ ] its failure to comply with PCI DSS standards, and allowing its computer systems to be breached, Defendant knowingly divulged consumer credit and debit account information, which was carried and maintained on Defendant's [RCS], and which allowed unauthorized third parties to duplicate consumers' credit cards[,]" in violation of 18 U.S.C. § 2702(a)(2)(A). [Id. ¶¶ 110, 111]. Defendant argues that it is neither an ECS nor an RCS, that it does not provide service "to the public," that the data which it transmits for merchants is not the "contents of a communication," and that Defendant did not "knowingly divulge" any protected information. [Doc. 23-1 at 12].

In support of their argument that Defendant is an ECS, Plaintiffs argue that Defendant "acts just like a phone company, ISP, or email provider by being in the business of operating the conduit by which electronic communications are transmitted" and that, as alleged in the FAC, "[t]hrough its payment processing equipment, [Defendant] . . . enable[s] consumers to send wire or electronic communications concerning their accounts and PII to financial institutions processing their credit card and other electronic payments." [Doc. 27 at 13-14, citing FAC ¶ 23, 26, 102]. The SCA defines an ECS as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. §2510(15). In Steiger, the

Eleventh Circuit held that an ECS under "[t]he SCA clearly applies, for example, to information stored with a phone company, Internet Service Provider (ISP), or electronic bulletin board system (BBS)." Id., 318 F.3d at 1049.[11]

"[C]ourts have consistently acknowledged that internet service providers, e-mail service providers, and telecommunication companies also provide electronic communication services under the SCA." In re Michaels Stores Pin Pad Litigation, 830 F. Supp. 2d 518, 523 (N.D. Ill. 2011) (hereinafter referred to as the Michaels case).[12]

---

[11]Steiger dealt with a claim under 18 U.S.C.§ 2702(a)(3), which, like §§ 2702(a)(1) and (a)(2), applies to communications knowingly divulged by an RCS or ECS but divulged to governmental entities rather than to any person or entity. The Eleventh Circuit held that § 2702(a)(3) of the SCA was not violated when an anonymous source provided information to police by hacking into Steiger's personal computers to retrieve child pornography because there was no evidence to suggest that Steiger maintained an "electronic communication service." The court went on to state in *dicta* that the SCA "may apply to the extent the hacker accessed and retrieved any information stored with [the computer owner's] Internet service provider." Steiger, 318 F.3d at 1049.

[12]The cases cited by the court included: Steinbach v. Village of Forest Park, 2009 WL 2605283, at *5 (N.D. Ill. August 25, 2009) ("finding that the Village of Forest Park did not provide [an ECS] because it provided an e-mail address but not the e-mail or internet service"); United States v. Weaver, 636 F. Supp. 2d 769, 769-70 (C.D. Ill. 2009) ("noting that Microsoft, the internet and e-mail service provider, provided electronic communication services and remote computing services"); Terkel v. AT & T Corp., 441 F. Supp. 2d 899, 901-04 (N.D. Ill. 2006) ("assuming that AT & T, a telecommunications company providing telephone and internet services, provides

In Michaels, the retailer reported in May 2011 that PIN pad tampering may have occurred in its Chicago area stores, and it later revealed that skimmers[13] had placed approximately ninety tampered PIN pads in eighty stores across twenty states between February and May 2011. Id. at 522. This occurred at a time when Michaels was not compliant with PCI PIN Security Requirements. Id. The court found, however, that "the alleged data breach has nothing to do with the provision of [an ECS] because the skimmers obtained the information from the mere swipe of the card on the PIN pad and not when the underlying service transmitted the information to a third party for

---

electronic communication services"); Andersen Consulting LLP v. UOP, 991 F. Supp. 1041, 1043 (N.D. Ill. 1998) ("concluding that defendant who did not provide internet services did not provide electronic communication services by maintaining an internal e-mail system"). See Michaels, 830 F. Supp. 2d at 523.

[13]"Michaels accepts customer payments for purchases through credit and debit cards . . . such as Visa USA ('Visa'). Some card issuers, like Visa, contractually obligate merchants, like Michaels, to comply with various PIN pad security standards that protect customer financial information as a condition to processing transactions through the card issuer." Id. at 522. "One method skimmers use to obtain debit and credit card information from retail stores is referred to as PIN pad swapping . . . remov[ing] a legitimate PIN pad from a merchant's store and replac[ing] it with a modified PIN pad that captures [and] then stores the data for later physical retrieval by the skimmers or wirelessly transmits the data to the skimmers." Id. at 521-22 (internal quotation marks omitted).

approval."[14] Id. at 524. The Michaels court further found fatal to the plaintiffs' SCA ECS claim their failure to allege that Michaels "provide[d] the internet or phone service through which the PIN pad communicates." Id. "Ultimately," the court held, "the provider of an [ECS] is the provider of the underlying service which transports the data, such as an internet service provider or a telecommunications company whose cables and phone lines carry internet traffic, and not the provider of a product or service which facilitates the data transport." Id.

Defendant argues that Plaintiffs' FAC, like the complaint in Michaels, fails to allege that Defendant "provides phone, internet, or interactive communication service" [Doc. 23-1 at 13], that Global Payments "provides payment processing service which, exactly like *In re. Michaels*, utilizes an internet service provider[,]" and that Plaintiffs cannot point to a single case where a payment processor, such as Defendant, was found to be an ECS [Doc. 29 at 7, 8]. Plaintiffs contend that they have avoided the fatal pleading error in Michaels and sufficiently alleged that Defendant provides the

[14]Michaels was not an RCS because the plaintiffs failed to demonstrate that the retailer either provided off-site computer storage or computer processing services. Id. A person or entity is also not an RCS when any storage of information is incidental to the main service provided by the defendant to its employees or customers. See Burrows v. Purchasing Power LLC, No. 1:12-cv-22800, Doc. 37 at 11-12 (S.D. Fla. October 18, 2012) (citing In re Jet Blue, 379 F. Supp. 2d at 310)). [A copy of the Burrows decision can be found at Doc. 29, Exhibit A].

underlying service transmitting Plaintiff's data. In support, Plaintiffs cite their allegation that Defendant "'provides consumers with payment processing services that enable consumers to send wire or electronic communications concerning their accounts and PII to financial institutions processing credit card and other electronic payments'" [Doc. 27 at 13-15, quoting FAC ¶ 102], mirroring the plaintiffs' allegation in Michaels, see 830 F. Supp. 2d at 524. Plaintiffs also cite their allegations that, as a merchant acquirer, Defendant forwards Plaintiff's PII and that Defendant's services include "acquiring front-end network . . . and an array of Internet-based solutions for payment processing and storefront enablement." [FAC ¶¶ 23, 26].

The question before the court is whether the FAC states a plausible claim that Defendant provides the underlying service which transports the data. Based on the holding in Michaels, if Global Payments utilizes a third-party internet service provider as it contends, Defendant is not an ECS provider. Accord Steinbach, 2009 WL 2605283, at *7 (holding the Village of Forest Park was not an ECS provider because, while it provided an email address, the Village "purchase[d] Internet access from a third-party provider"). Defendant points out that Plaintiffs' "own allegations [are] that Defendant is a credit card processor" and "[a]t no point in the FAC do Plaintiffs allege

that Global Payments is the provider of the underlying internet service." [Doc. 29 at 8, citing FAC ¶¶ 19, 21, 26, 36-40, 102, 104].

Regardless of whether Plaintiffs have already or could replead the FAC to state a plausible claim against Global Payments as an ECS or RCS, which the court need not decide, the FAC fails to state an SCA claim for other reasons. Plaintiffs have not pled facts demonstrating that Defendant provides a service "to the public" or that Defendant "knowingly divulged" Plaintiffs' data, and repleader on these SCA requirements would be futile.

Courts addressing the SCA requirement that the relevant service be offered "to the public" have held that the "unambiguous," plain meaning of the word public is "'the community at large.'" See H Group, Inc., 2012 WL 195724, at *6 (quoting Andersen Consulting, LLP, 991 F. Supp. at 1042). The legislative history of the SCA states that "'[e]lectronic mail systems may be available for public use or may be proprietary, such as systems operated by private companies for internal correspondence.' . . . Thus, [the plaintiff] must show that [the defendant's] electronic mail system was available for public use.'" Andersen Consulting, LLP, 991 F. Supp. at 1042-43 (quoting S. Rep. No. 99–541, at 8 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3562).

Plaintiffs' conclusory allegation that Defendant provides an ECS "to the public" is not supported by the allegations in the FAC. Defendant, a "merchant acquirer," offers its services to the merchants with which it has a contract, i.e., to *its* customers, not to the "community at large." See Burrows, No. 1:12-cv-22800, Doc. 37 at 11-12 (conclusory allegation of services to the public insufficient to state SCA claim); and see H Group, Inc., 2012 WL 195724, at **1, 6 (granting motion to dismiss where services were not offered to the public, they were developed to provide "back office operations, . . . which include a technological infrastructure for computer services, server access for storing client files and other files, and providing email to the [*defendant's*] Advisor Affiliates . . . and to . . . [*its*] outside advisors") (internal quotation marks omitted).

The FAC also fails to plead facts stating a claim that Defendant "knowingly divulged" Plaintiffs' PII. As Defendant points out, the legislative history of the SCA states:

> The term knowingly means that the defendant was aware of the nature of the conduct, aware of or possessing a firm belief in the existence of the requisite circumstances and an awareness or a firm belief about the substantial certainty of the result. The conduct in question is the *act* of disclosure.

[See Doc. 23 at 17 (quoting H.R. Rep. No. 99-647, at 64 (1986))] (emphasis added). In Worix v. MedAssets, Inc., 869 F. Supp. 2d 893 (N.D. Ill. 2012), Worix asked the court to reconsider its dismissal of his SCA claim. The court had previously held that "whether information had been 'knowingly divulge[d]' should be analyzed according to 'the common meaning of knowing conduct[, which] includes willful blindness, but not recklessness or negligence.'" Id. (citation omitted).[15] And the court had concluded that "the failure to take reasonable steps to safeguard data, which was all that Worix had alleged, [did] not, without more, amount to divulging that data knowingly or with

---

[15] Accord Freedman v. America Online, Inc., 329 F. Supp. 2d 745, 748-49 (E.D. Va. 2004). Discussing "knowingly" as that term is used in § 2702(a)(3), the court found that:

> [P]ertinent legislative history provides that "knowingly means that the defendant was [(i)] aware of the nature of the conduct, [(ii)] aware of or possessing a firm belief in the existence of the requisite circumstances and [(iii)] an awareness [sic] of or a firm belief about the substantial certainty of the result." H.R. Rep. No. 99-647, at 64 (1986). The legislative history further clarifies what a plaintiff must show to establish each of these three prongs and thus show that defendant "knowingly divulge[d]" plaintiff's subscriber information. . . . And, . . . with regard to the third prong, plaintiff must show that defendant was aware, or possessed a firm belief, that his *act* would result in the disclosure of the subscriber information to another person or entity. See id. ("The result is that the contents have been *provided* to another person or entity.").

Id. at 748 (emphasis added).

willful blindness." 869 F. Supp. 2d at 896 (citation and internal quotation marks omitted). Worix argued that the court had erred in dismissing his claim at the pleading stage when evidence procured during the discovery phase might provide proof that the defendant "took deliberate actions to turn a blind eye to the critical security threat created by its lax practices." Id. (citation and internal quotation marks omitted). But the court rejected that argument because, as it had explained in its previous decision, Worix had not alleged "an actual *act*" by the defendant, "only that [the defendant's] actions created or contributed to an unacceptable *risk* that data would be compromised." Id. (emphasis in original).

Likewise, Plaintiffs have not alleged any *act* by Defendant Global Payments, only that Defendant, which was PCI DSS compliant at the time, somehow created or contributed to the breach of its data system. The case law cited by Defendant demonstrates that, contrary to Plaintiffs' allegations and argument, the fact that Visa and Mastercard removed Global Payments from their lists of "PCI DSS compliant" companies in the wake of the data theft is not evidence that Defendant violated the SCA. [See Doc. 23-1 at 18 n.3, citing *inter alia* Edwards v. Toys "R" Us, 527 F. Supp. 2d 1197, 1204 n.11 (C.D. Cal. 2007) (discussing cases finding that prior *non*-compliance would be relevant in proving willfulness but indicating that the fact of

prior compliance would not be indicative of a lack of willfulness on the defendant's part)]. Plaintiffs have not cited any case holding otherwise.

For the above reasons and authority, the court **RECOMMENDS** that Plaintiffs' SCA claims (Count II) be **DISMISSED WITH PREJUDICE**.

B. FCRA Claims

Plaintiffs third and fourth causes of action are claims that Defendant is a "consumer reporting agency" and willfully and negligently violated 15 U.S.C. § 1681(b) of the FCRA by "failing to adopt and maintain reasonable procedures . . . to adequately secure its servers and computer storage systems . . . while maintaining the confidentiality . . . of" Plaintiffs' personal information.[16] [FAC (Count III) ¶ 122; FAC (Count IV) ¶ 129]. The statute cited in the FAC states that the purpose of the FCRA is "to require that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information in

[16]A defendant who negligently violates the FCRA is liable for any actual damage sustained by the plaintiff, 15 U.S.C. § 1681o(a)(1). Willfulness as used in 15 U.S.C. § 1681n, under which a defendant can also be liable for punitive damages, means the defendant acted with knowledge or recklessness.

accordance with the requirements of this subchapter." 15 U.S.C. § 1681(b). Plaintiffs allege that Defendant is, therefore, "required to adopt and maintain reasonable procedures for meeting the needs of commerce . . . while maintaining the confidentiality . . . of [the consumer's] information" [FAC, ¶ 120], that Defendant "may only *furnish* a consumer report to another person for a permissible purpose" [id. ¶ 121 (emphasis added)], and that "because of [Defendant's] failure to maintain reasonable procedures, hackers gained unauthorized access to consumer report information absent a permissible purpose" [id. ¶ 122]. Global Payments argues that the FCRA claims should be dismissed because Defendant did not violate the FCRA by "furnishing" Plaintiffs' data and does not provide consumer reports or act as a consumer reporting agency as defined by the FCRA. [Doc. 23-1 at 18-24].

Defendant argues that Global Payments did not furnish Plaintiff's personal data to hackers; rather, the data was stolen. [See Doc. 23-1 at 20, citing *inter alia* Holmes v. Countrywide Fin. Corp., 2012 WL 2873892, at *16 (W.D. Ky. July 12, 2012) (holding that plaintiffs failed to state an FCRA claim against defendant where defendant's employee "independently stole [defendant's] customer information"); Doc. 29 at 12-13]. Plaintiffs' attempt to distinguish Holmes by arguing that their data was stolen by "*unrelated* third parties," not by an employee of Defendant [Doc. 27 at 21

(emphasis added)], draws a distinction, but it is a distinction that has no legal significance to Plaintiffs' FCRA claims.

The relevant fact is that the data was stolen, not furnished. The FCRA provides that a consumer reporting agency "may *furnish* a consumer report under [only certain] circumstances and no other . . . . " 15 U.S.C. § 1681b (emphasis added). The FCRA does not define the word "furnish." But, as the cases cited by Defendant demonstrate, "furnish," as used in the FCRA, involves the act of "transmit[ting] information" to another. [Doc. 23-1 at 19-20, citing *inter alia* Holmes, 2012 WL 2873892, at *16]. And, as Defendant points out, the FCRA requirement to "maintain reasonable procedures," which is found under 15 U.S.C. § 1681e, is "designed to . . . limit the *furnishing* of consumer reports to the purposes listed under section 1681b of this title. . . ." [Doc. 23-1 at 20 (emphasis added)].[17] Defendant argues -- without any counter argument from Plaintiffs -- that because Defendant did not transmit or furnish data to the hackers, it therefore did not violate the reasonable procedures requirement in § 1681e. [Id., citing Washington v. CSC Credit Servs. Inc., 199 F.3d 263, 267 (5th Cir. 2000) (reversing the district court and holding that "a plaintiff bringing a claim that a

[17]Plaintiffs do not cite 15 U.S.C. § 1681e in the FAC, but as Defendant points out, the statute is clearly relevant to the premise behind Plaintiffs' FCRA claims.

reporting agency violated the 'reasonable procedures' requirement of 1681e must first show that the reporting agency released the report in violation of 1681b")].

Defendant further argues that it is not a "consumer reporting agency" and does not provide "consumer reports" as defined by the FCRA. Plaintiffs allege that Global Payments is a consumer reporting agency because, in addition to being a card processor, Global Payments "collects, analyzes and retains information bearing on consumers' credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or modes of living[and t]hrough such products as its 'Global Access @dvantage,' . . . makes [such] information . . . available for use by third parties." [FAC ¶¶ 27, 117-119]. "The term 'consumer reporting agency' means any person which, for monetary fees, . . . regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers *for the purpose of furnishing consumer reports to third parties*, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports." 15 U.S.C. § 1681a(f) (emphasis added). The FCRA "applies only to 'consumer reports' which are used for consumer purposes; '[i]t does not apply to reports utilized for business, commercial or professional purposes.'" McCready v. eBay, Inc., 453 F.3d 882, 889 (7th Cir. 2006) (quoting Ippolito v. WNS,

Inc., 864 F.2d 440, 452 (7th Cir. 1988) (citations omitted) (emphasis removed)). And Defendant argues that its Access@dvantage service is not a consumer credit report to a third party; rather it is "a service offered by [Defendant] to merchants that allows merchants to review and analyze *their own* transaction history [and] in no way [can any information] be linked with a specific consumer or . . . used to make any credit related or similar decision related about a consumer." [Doc. 23-1 at 24-25; Exhibit A, the Declaration of Kristine M. Brown, attaching true and correct copies of Defendant's webpages]. Plaintiffs acknowledge that the consumer reports which Global Payments creates "were not themselves necessarily within the scope of the data breach" at issue in this action [Doc. 27 at 22] and have not directly responded to Defendant's arguments that it does not offer consumer reports and is not a consumer reporting agency. See also Holmes, 2012 WL 2873892, at *15 ("Courts construing who or what qualifies as consumer reporting agencies have restricted the label to the credit reporting bureaus.").

The undersigned accordingly **RECOMMENDS** that Plaintiffs' FCRA claims (Counts III and IV) be **DISMISSED WITH PREJUDICE**.

C. State Law Claims

1. Georgia Unfair and Deceptive Trade Practices Act

In Count V, Plaintiffs claim that Defendant violated the Georgia UDTPA, O.C.G.A. §§ 10-1-372(a)(5) and (7), by "[mis]represent[ing] among other things, that it has 'one of the safest, most secure transaction processing systems in the world [and] provides hacker-resistant . . . processing that customers can trust and rely on.'" [FAC ¶¶ 144, 145]. The FAC also alleges that Defendant violated the UDTPA, O.C.G.A. § 10-1-372(a)(12), by not notifying affected customers of the nature and extent of the data breach and thus "created a likelihood of confusion or misunderstanding . . . preventing those customers from taking reasonable measures to protect against the threat of continued and future injury." [Id. ¶ 146].

Choice of Law

Defendant argues that "Georgia's choice of law rules prevent Plaintiffs from asserting a claim under the UDTPA because Plaintiffs' alleged injuries occurred outside of Georgia." [Doc. 23-1 at 26]. "'Georgia continues to apply the traditional choice of law principles of *lex loci delicti*'" in tort actions. nVision Global Technology Solutions, Inc. v. Cardinal Health 5, LLC, -- F. Supp. 2d --, 2012 WL 3527376, at *27 (N.D. Ga. August 14, 2012) (citation omitted). "[T]he rule of *lex loci*

delicti [ ] requires application of the substantive law of the place where the tort or wrong occurred." Carroll Fulmer Logistics Corp. v. Hines, 309 Ga. App. 695, 696, 710 S.E.2d 888, 889 (2011). "[T]he place of the wrong is where the injury was sustained and not where the last act causing the injury occurred." Mullins v. M.G.D. Graphics Systems Group, 867 F. Supp. 1578, 1580 (N.D. Ga. 1994). Defendant argues that the *lex loci delicti* rule requires the court to apply Kansas and California law to Plaintiffs' respective tort claims. [Doc. 23-1 at 27; Doc. 29 at 17]. Plaintiffs argue that "Georgia's interest in regulating the conduct of [Global Payments] dictates applying the UDTPA to Plaintiffs' claims" because Defendant's principal place of business is in Georgia, the data breach occurred in Georgia, and Defendant's decision to withhold information regarding the nature and extent of the breach from affected consumers occurred in Georgia. [Doc. 27 at 22-23]. The court will apply Georgia law.

Defendant has overlooked the exceptions to the rule of *lex loci delecti*. "Although the rule in Georgia is *lex loci delicti*, there are exceptions if the *lex loci delicti* is foreign law. One exception is the application of common law. Foreign law does not apply if no foreign statutes are involved. If the parties do not identify any foreign statutes in their pleadings, it is presumed that no foreign statutes are involved." In re Stand 'n Seal, Products Liability Litigation, 2009 WL 2998003, at *2 (N.D. Ga.

September 15, 2009) (citations and internal quotation marks omitted). Defendant has not identified a Kansas or California statute or rule of law which would apply to Plaintiffs' Count IV claims; therefore, the court need not apply a foreign law.

Also, applying foreign law in this case would contravene Georgia's public policy interest in regulating Defendant's conduct.

> Even if an application [of the rule of *lex loci delicti*] renders the law of another state applicable, the forum, within constitutional limits, is not required to give the law of another state extra-territorial effect. That is only done as a matter of courtesy or comity, which will not be enforced if the law of the other state contravenes the public policy of the forum. See OCGA § 1-3-9; Commercial Credit Plan v. Parker, 152 Ga. App. 409, 263 S.E.2d 220 (1979).

Fed. Ins. Co. v. Nat. Distrib. Co., Inc., 203 Ga. App. 763, 766, 417 S.E.2d 671, 674 (1992). As Plaintiffs argue, Defendant's principal place of business is in Georgia, the data breach occurred in Georgia, and to the extent, if any, Defendant breached a duty to consumers, it did so in Georgia. The court will therefore consider whether Plaintiffs have stated a claim against Defendant under the Georgia UDTPA.

UDTPA Claims

Plaintiffs claim that Defendant's representations regarding its services, such as, that it that offers "hacker-resistant" transaction processing, are misrepresentations in violation of O.C.G.A. §§ 10-1-372(a)(5) and (7), and that by failing to notify affected

customers of the nature and extent of the data breach and instead looking to the individual card issuing institutions to monitor the breached accounts for fraudulent activity, Defendant "created a likelihood of confusion or misunderstanding . . . preventing [ ] customers from taking reasonable measures to protect against the threat of continued and future injury" in violation of O.C.G.A. § 10-1-372(a)(12). [FAC ¶¶ 32, 146]. Misrepresentations which are deceptive trade practices under the UDTPA include representations "that goods or services have . . . characteristics . . . [or] benefits . . . that they do not have" and representations "that goods or services are of a particular standard, quality, or grade . . . if they are of another." O.C.G.A. § 10-1-372(a)(5), (a)(7). And "[a] person [who] . . . in the course of his business . . . [e]ngages in any [ ] conduct which . . . creates a likelihood of confusion or of misunderstanding" has engaged in a deceptive trade practice. O.C.G.A. § 10-1-372(a)(12). Plaintiffs seek "injunctive relief . . . including, but not limited to, . . . properly notifying Plaintiffs and Class Members of . . . the extent of the breach, providing credit monitoring and identity theft protection, and implementing proper safeguards to prevent a future data breach." [FAC ¶ 150; Doc. 27 at 27].

Defendant argues that Plaintiffs' misrepresentation claims are not supported by the factual allegations in the FAC and that Plaintiffs have failed to allege any future

harm that could be redressed by an injunction against Defendant. [Doc. 23-1 at 27]. As discussed *infra* in the context of Plaintiffs' claims for negligence, the fact that Defendant's system was hacked does not create an inference that Defendant was negligent; nor does the data theft create an inference that Defendant misrepresented its services. Moreover, Plaintiffs' UDTPA claims fail to state a claim against Defendant for which relief can be granted because Plaintiffs have not alleged facts showing that they are likely to be harmed absent injunctive relief.

Injunctive relief is the sole remedy under the UDTPA. See Catrett v. Landmark Dodge, Inc., 253 Ga. App. 639, 644, 560 S.E.2d 101, 106 (2002) (citing O.C.G.A. § 10-1-373(a)). "[T]o be entitled to injunctive relief, a plaintiff must establish that he is '[a] person likely to be damaged by a deceptive trade practice of another.'" Moore-Davis Motors, Inc. v. Joyner, 252 Ga. App. 617, 619, 556 S.E.2d 137, 140 (2001) (quoting O.C.G.A. § 10-1-373(a)). That is, Plaintiffs must show that they are "likely to be damaged in the future by some deceptive trade practice of [Defendant]." Bolinger v. First Multiple Listing Service, Inc., 838 F. Supp. 2d 1340, 1364 (N.D. Ga. 2012) (citation and internal quotation marks omitted). Injunctive relief is available under the UDTPA "without proof of monetary damage, loss of profits or intent to deceive." BellSouth Corp. v. Internet Classifieds of Ohio, 1997 WL 33107251, at *24

(N.D. Ga. November 12, 1997) (citing O.C.G.A. § 10-1372(a)). However, "'[a] plaintiff who demonstrates past harm, but does not allege ongoing or future harm, has not shown that he is likely to be damaged within the meaning of section 10-1-373(a).'" Bolinger, 838 F. Supp. 2d at 1364 (quoting Silverstein v. Procter & Gamble Mfg. Co., 2008 WL 4889677, at *4 (S.D. Ga. November 12, 2008)).

Plaintiffs have not pled that they read, relied upon and, thus, were harmed by Defendant's "representations" and, even if they could replead such facts, Plaintiffs could, at most, demonstrate only past harm which is not a basis for injunctive relief under the UDTPA. Plaintiffs argue that they have sufficiently alleged future harm to support a UDTPA, O.C.G.A. § 10-1-372(a)(12), claim because Global Payments "has . . . inappropriately [ ] delegated their obligation under O.C.G.A. § 10-1-910 to what [Defendant] refers to as 'appropriate industry parties.'" [Doc. 27 at 26-27]. But, as Defendant has argued, "not a single provision of [the UDTPA] even suggests [that Defendant has] an affirmative duty to provide notification in a situation like the one Plaintiffs allege here." [Doc. 29 at 16].

The notice requirement cited by Plaintiffs, in O.C.G.A. § 10-1-910, is not part of the UDTPA -- it is part of the Security Breach of Computerized Personal Information Act ("SBCPIA") found under Title 10, Chapter 1, Article 34, enacted in

2005.[18] In the SBCPIA, the General Assembly, responding to the fact that the "privacy and financial security of individuals is increasingly at risk due to the ever more widespread collection of personal information by both the private and public sectors," declared in pertinent part that:

> (7) Victims of identity theft must act quickly to minimize the damage; therefore, expeditious notification of unauthorized acquisition and possible misuse of a person's personal information is imperative.

O.C.G.A. §§ 10-1-910(1), (7). However, the SBCPIA only requires that notice be given "*to any resident of this state* whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." O.C.G.A. § 10-1-912(a) (emphasis added). Plaintiffs are not residents of "this state." Thus, even if Plaintiffs intended to state a claim for relief based on the Security Breach of Computerized Personal Information Act, they have failed to do so.

And the FAC fails to state a claim for relief under the UDTPA because Plaintiffs' allegations of future harm are based entirely on speculation of an increased risk of identity theft, and speculation about future harm is insufficient to sustain a UDTPA claim. See Byung Ho Cheoun v. Infinite Energy, Inc., 363 Fed. Appx. 691,

---

[18]The UDTPA, found in Title 10, Chapter 1, Article 15 of the OCGA, was enacted in 1968.

695 (11th Cir. 2010) (affirming district court's dismissal of UDTPA claim where plaintiff alleged only "hypothetical future harm") (citing Wiggin v. Horne, 270 Ga. 571, 572, 512 S.E.2d 247, 248 (1999) ("'Allegations of mere speculative or contingent injuries, with nothing to show that in fact they will happen, are insufficient to support a prayer for injunctive relief.'")).

The Bolinger case cited by Plaintiffs in support of their claim for future injury is factually inapposite. [Doc. 27 at 26, citing Bollinger, 838 F. Supp. 2d at 1364]. In Bollinger, the court held that the plaintiffs, buyers and sellers of residential property, had a plausible claim for relief under § 10-1-372(a)(12) because they faced a threat of future injury if the defendants failed to disclose hidden fees and kickbacks relating to broker compensation in home sales. Id. As argued by Defendant, unlike the relief given in Bollinger which would prevent future injury, an injunction against Global Payments would do nothing to change the data theft by hackers in the past and "would not prevent the thieves from misusing any stolen information" in the future. [Doc. 23-1 at 31]. Nor would an injunction redress any past harm from any alleged misrepresentation regarding the benefits or quality of Defendant's services. For the above reasons and authority, the court **RECOMMENDS** that Plaintiffs' O.C.G.A. §§ 10-1-372(a)(5), (a)(7) & (12), UDTPA claims be **DISMISSED WITH PREJUDICE.**

2. Negligence

Count I of the FAC is a claim that Defendant negligently breached a duty to protect Plaintiffs' PII as demonstrated by Defendant's alleged "failure to comply with PCI DSS standards" and removal from Visa's and Mastercard's lists of PCI DSS compliant payment processors. [FAC (Count I) ¶¶ 80-85]. Plaintiffs allege that, once Global Payments received Plaintiffs' PII, Defendant "assumed a duty, or had one imposed on it, to use reasonable care . . . and . . . commercially reasonable standards" to keep their PII private and secure [id. ¶ 81] and that Defendant had a "duty to publicly disclose the Data Breach in a timely manner pursuant to O.C.G.A. §§ 10-1-910-912 and similar data breach notification statutes in other states[.]" [FAC ¶ 87 & n.10 (citing, *inter alia*, Cal. Civ. Code 56.06, 1785.11.2, 1798.29, 1798.82; Kan. Stat. 50-7a01 &7102)].[19]

---

[19]The foreign statutes cited in passing by Plaintiffs in a footnote to the FAC do not give Plaintiffs a cause of action for negligence under the facts in this action. The Kansas statutes cited by Plaintiffs [FAC at 30 n.10] allow for "substitute notice" of a data breach which can include "conspicuous posting of the notice on the web site page of the individual or the commercial entity if the individual or the commercial entity maintains a web site; and [ ] notification to major statewide media[,]" K.S.A. § 50-7a01(e)(2)-(3), and apply to persons or entities conducting business in Kansas, K.S.A. § 50-7a02. The California statutes cited by Plaintiffs regulate medical information (Cal. Civ. Code § 56.06), a consumer's or credit reporting agency's election to place a security freeze on the consumer's credit report (id. § 1785.11.2), and the notice of a data breach, but the latter statute, like Kansas, provides for "substitute notice" when

Plaintiffs concede that regardless of which state law is applied, the requirements for a negligence cause of action are the same: (1) a duty owed by the defendant; (2) breach of that duty; (3) causation; and (4) injury or damages. [Doc. 27 at 30-31]. "Plaintiffs . . . chose to file . . . here. They will be tried here." In re Stand 'n Seal, 2009 WL 2998003, at *3. And the court will apply Georgia law to Plaintiff's negligence claims.

Plaintiffs' O.C.G.A. §§ 10-1-910, *et seq*., negligence claim is subject to dismissal for the same reason discussed *supra* in the context of Plaintiffs' UDTPA claim -- the statute only requires giving notice to residents of Georgia, and Plaintiffs are not Georgia residents And the cases cited by Defendant demonstrate that courts have found that no duty of care exists in the data breach context where, as here, there is no direct relationship between the plaintiff and the defendant. [See Doc. 29, citing Hammond, 2010 2643307, at *9; Worix, 2012 WL 1419257, at **3-6]. The cases cited by Plaintiffs are factually distinguishable and, thus, do not support Plaintiffs' negligence claims. In each case cited by Plaintiffs, the claimant had a direct relationship with the defendant and, therefore, had a basis for claiming that the

---

the affected class of person exceeds 500,000 (id. §§ 1798.29(i)(3)(A)-(C); 1798.82(3)(A)-(C)). Thus, the statutes cited fail to provide a cause of action for negligence for Plaintiffs in this action.

defendant owed a duty of care. For example, the plaintiffs in AvMed, Inc., 2012 WL 3833035, at *1, were the defendant's customers, and the plaintiff in Anderson v. Hannaford Bros. Co., 659 F.3d 151, 159 (1st Cir. 2011), was a customer of the grocery store defendant. In RockYou, the plaintiffs were the users of applications suing the application developer to whom they had directly provided their PII. Id., 785 F. Supp. 2d at 866. And, in RBSW, the court never reached the question of duty as to Badish, who, like Plaintiffs, had no direct relationship with the defendant.[20]

Plaintiffs argue that Defendant had a duty to protect their PII under the "voluntary undertaking doctrine." [Doc. 27 at 32]. Under Georgia law, "a person may be held liable for the negligent performance of a voluntary undertaking" -- that is, "'one who undertakes to do an act or perform a service for another has the duty to exercise care, and is liable for injury resulting from his failure to do so, even though his undertaking is purely voluntary . . . completely gratuitous . . . or there was no consideration for the promise or undertaking sufficient to support an action *ex contractu* based thereon.'" Osowski v. Smith, 262 Ga. App. 538, 540, 586 S.E.2d 71,

[20]However, the court held that the plaintiff, Irwin, who suffered actual identity theft, had stated a claim for negligence. The court did not provide substantive analysis on the issue of duty. But RBSW, at the request of Irwin's bank, had issued Irwin a gift card.

73 (2003) (citation omitted). However, the voluntary undertaking doctrine is available only to a plaintiff who has suffered "physical harm." See Huggins v. Aetna Cas. & Sur. Co., 245 Ga. 248, 248, 264 S.E.2d 191, 192 (1980) (citing the majority rule as stated in the Restatement 2d Torts § 324A). Plaintiffs do not allege that they have suffered physical harm; therefore, they cannot state a negligence claim based on the voluntary undertaking doctrine.

Defendant argues that Plaintiffs' negligence action would be barred by the "economic loss doctrine" if the FAC states a claim for breach of contract. [Doc. 29 at 19, citing City of Cairo v. Hightower Consulting Eng'rs, Inc., 278 Ga. App. 721, 629 S.E.2d 518 (2006)]. "The economic loss rule generally provides that a contracting party who suffers purely economic losses must seek his remedy in contract and not in tort [and that] a plaintiff can recover in tort only those economic losses resulting from injury to his person or damage to his property[.]" City of Cairo, 278 Ga. App. at 728, 629 S.E.2d at 525 (citation and internal quotation marks omitted). Courts addressing data breach cases have dismissed negligence claims based on the economic loss doctrine where the plaintiff has not suffered personal injury or property damage. See, e.g., Michaels, 830 F. Supp. 2d at 531(dismissing negligence and negligence *per se* claims); accord In re Heartland Payment Sys., Inc., Customer Data Sec. Breach Litig.,

834 F. Supp. 2d 566, 590 (S.D. Tex. 2011) (dismissing negligence claim with prejudice and without leave to amend because amendment would be futile).

And Plaintiffs' allegation that Defendant has negligently breached a "duty to utilize commercially reasonable methods to safeguard Plaintiffs' PII and to comply with industry standards required for payment processors [FAC ¶ 81; Doc. 27 at 32] is also without merit. Defendant points out that "Plaintiffs cite no case law that would support a finding that commercial standards or general industry standards such as PCI-DSS would create a legal duty running from GP to Plaintiffs." [Doc. 29 at 20; Doc. 23-1 at 18 n.3]. And, as discussed *supra* in the context of Plaintiffs' SCA claims, courts have held only that prior *non*-compliance is relevant in proving willfulness. See Toys "R" Us, 527 F. Supp. 2d at 1204 n.11 (discussing cases). "It is well established that the occurrence of an unfortunate event is not sufficient to authorize an inference of negligence." Johnson v. MARTA, 230 Ga. App. 105, 106, 495 S.E.2d 583, 584 (1998) (citations and internal quotation marks omitted).

For the reasons and authority discussed, the court **RECOMMENDS** that Plaintiffs' negligence claims (Count I) be **DISMISSED WITH PREJUDICE**.

3. Contract Claims

The last two claims in the FAC are for "Breach of Third Party Beneficiary Contract" (Count VI) and "Breach of Implied Contract" (Count VII). Defendant argues that Plaintiffs "fail to identify the contracts at issue or *inter alia* where they were made" and that Plaintiffs fail to state a claim for which relief can be granted under Kansas, California and Georgia law. [Doc. 23-1 at 37 n.15, 39]. Plaintiffs argue that there is no conflict between Kansas and California law but that application of Georgia's laws to the contract claims is "appropriate and constitutionally permissible." [Doc. 27 at 29-30].

Choice of Law

"In contract actions, Georgia courts apply the traditional *lex loci contractus* rule: a contract is governed as to its nature, validity and interpretation by the law of the state where the contract was made, unless it appears from the contract itself that the contract was to be performed in another state." Rayle Tech, Inc. v. DEKALB Swine Breeders, Inc., 897 F. Supp. 1472, 1475 (1995) (citing General Telephone Co. of Southeast v. Trimm, 252 Ga. 95, 96, 311 S.E.2d 460, 462 (1984)). As argued by Plaintiffs, Defendant's alleged contractual obligation, if any, to Plaintiffs was breached not where Plaintiffs swiped their cards, as in the Michaels case, but, rather, where Defendant

performed its data transmission service, which Plaintiffs contend is Georgia where Defendant's principal place of business is located, the data breach occurred, and Defendant was allegedly obligated to safeguard Plaintiffs' PII from being stolen. [Doc. 27 at 22, 35]. The court will apply Georgia law.

Third Party Beneficiary Contract

Under Georgia law, O.C.G.A. § 9-2-20(b) provides that a third party may maintain an action against the promisor on the contract to which he was not a party; "[h]owever, . . . to have standing to enforce [the] contract . . . it must *clearly appear* from the contract that it was intended for his benefit." Haldi v. Piedmont Nephrology Assoc., P.C., 283 Ga. App. 321, 322-23, 641 S.E.2d 298, 300 (2007) (citation and internal quotation marks omitted) (emphasis added). "The mere fact that [a third party] would benefit from performance of the agreement is not alone sufficient. It must appear that both parties to the contract intended that the third person should be the beneficiary." Id. (citation and internal quotation marks omitted); accord Holland v. Levy Premium Foodservice Ltd. Partnership, 469 Fed. Appx. 794, 797 (11th Cir. 2012).

Plaintiffs argue that "it cannot be said that the processing contracts, on their face, do not require [Global Payments] to 'render some performance' to third party beneficiaries[,]" a confusing double-negative argument that misses the point made by

the court in Haldi. As third parties to the contract, "it must *clearly* appear from the contract that it was intended for [Plaintiffs'] benefit." Haldi, 283 Ga. App. at 322-23, 641 S.E.2d at 300 (citation and internal quotations marks omitted) (emphasis added). The contract between Global Payments and its merchant acquirers is not before the court, but the court agrees with Defendant that "[t]he third-party beneficiary claim that this Court found sufficient . . . in RBSW demonstrates the patent inadequacy of Plaintiffs' allegations here." [Doc. 29 at 22-23].

In RBSW, the court held that the plaintiff Irwin had sufficiently stated a third-party beneficiary contract claim. Irwin's bank had contracted with RBSW to issue gift cards to the bank's customers, including Irwin, and then process the cards. In contrast, Global Payments has not issued anything directly to Plaintiffs. Defendant has processed data to assist its merchant clients when a customer attempts to make a purchase with a credit or debt card. The cases cited by Defendant demonstrate that, while consumers like Plaintiffs benefit from Defendant's service, they are not intended third party beneficiaries of the agreement between Global Payments and its merchants. See, e.g., Sovereign Bank v. BJ's Wholesale Club, Inc., 533 F.3d 162, 171 (3rd Cir. 2008) (noting with approval the district court's comment that "'an incidental beneficiary has no right to enforce a contract, no matter how great a stake it might

have in doing so'") (citation omitted); Lone Star Nat. Bank, N.A. v. Heartland Bank, Civil Action No. H-10-171, Order on Motion to Dismiss (S. D. Tex. March 31, 2011) (dismissing third-party beneficiary claim in data breach case);[21] Banknorth, N.A. v. BJ's Wholesale Club, Inc., 442 F. Supp. 2d 206, 211 (M.D. Pa. 2006) (denying third-party beneficiary claims for breach of agreement between merchant and its acquiring bank after a security breach; contract between merchant and bank expressly excluded third-party beneficiary status). [See Doc. 23-1 at 39; and see Doc. 29 at 23 (citations omitted)].

Implied Contract Claim

Plaintiffs' last cause of action, an "implied contract" claim, is "based in part on Defendant's public statements outlining its commitment to safeguard consumers' personal and financial information" and in part on Defendant's acceptance of Plaintiffs' sensitive PII: Plaintiffs allege that they "would not have provided their personal information to Defendant" if they had not believed that Defendant had an implied contractual obligation to Plaintiffs to safeguard their data. [FAC (Count VII) ¶¶ 174-76].

[21]A copy of the decision is attached to Doc. 29 as Exhibit B.

Defendant argues that Plaintiffs have not pled any basis for inferring that Global Payments and its merchants mutually intended to benefit Plaintiffs. [Doc. 23-1 at 39]. Plaintiffs did not provide their data to Defendant; as they allege in the FAC, they provided their card data to a merchant who in turn provided it to Defendant. [FAC ¶¶ 53, 61]. The FAC does not plead that Plaintiffs were aware of, much less relied upon, Defendant's statements about its services prior to submitting their data to a merchant. And the cases cited by Defendant support Defendant's argument that broad statements of reliance on a defendant's website and privacy statement do not give rise to contract claims where, as here, Plaintiffs do not allege that they read and relied upon those statements. [Doc. 29 at 24]. See Trikas v. Universal Card Servs. Corp., 351 F. Supp. 2d 37, 46 (E.D. N.Y. 2005) (dismissing contract claim for "breach of privacy promise" stating in *dicta* that "broad statements of company policy do not generally give rise to contract claims") (citation and internal quotation marks omitted); Dyer v. Northwest Airlines Corps., 334 F. Supp. 2d 1196, 1199-1200 (D. N.C. 2004) (dismissing breach of contract claim as a matter of law because "broad statements of company policy do not generally give rise to contract claims" and because plaintiffs did not allege that they had logged onto the defendant's website, read or relied upon the defendant's privacy policy and failed to allege any damages arising out of the

alleged breach of contract); In re Northwest Airlines Privacy Litig., 2004 WL 1278459, at **5-6 (D. Minn. June 6, 2004) (finding no contract where plaintiffs alleged they "relied to their detriment" on defendant's privacy policy but failed to allege that they actually read defendant's privacy statement prior to providing defendant with their personal information).

Plaintiffs argue that "whether an implied-in-fact contract exists is a factual inquiry inappropriate for resolution at the motion to dismiss stage" and that courts in data breach cases have allowed breach of implied contract claims to survive motions to dismiss. [Doc. 27 at 38, 39]. However, the cases cited by Plaintiffs are factually distinguishable and do not support Plaintiffs' argument. As Defendant argues, "the majority of the cases relied upon by Plaintiffs are [ ] distinguishable because they involved customers of the defendants who had provided their PII directly to the defendants." See, e.g., AvMed, Inc., 693 F.3d at 1322, 1327 (Plaintiffs were customers of AvMed, Inc., and, even then, the court stated, "Had Plaintiffs alleged fewer facts, we doubt whether the [implied contract claim] could have survived a motion to dismiss."); Hannaford Bros. Co., 659 F.3d at 159 (plaintiffs' breach of implied contract claim survived defendant's motion to dismiss because "a jury could reasonably conclude [ ] that an implicit agreement [by a store] to safeguard [its

customers'] data is necessary to effectuate the contract" that exists between them); RockYou, 785 F. Supp. 2d at 865) (breach of contract or breach of implied contract claims survived motion to dismiss where user sued the developer of online services and an application for use with social networking sites to which the user had directly submitted his PII); accord RBSW at 17 (allowing plaintiff Irwin's implied contract claim to survive motion to dismiss with little substantive discussion where Irwin's bank contracted for RBSW to issue a gift card to Irwin and process that card). Plaintiffs, in contrast, provided their PII to a merchant, not directly to Defendant, and Defendant was not asked to give anything to or do anything for Plaintiffs.

For the above reasons, the court **RECOMMENDS** that Plaintiffs' "third-party-beneficiary" (Count VI) and implied contract (Count VII) claims be **DISMISSED WITH PREJUDICE**.

IV. Conclusion

The court **RECOMMENDS** that Defendant's Rule 12(b)(6) motion [Doc. 23] to dismiss the complaint for failure to state a claim for which relief can be **GRANTED** and that the complaint be **DISMISSED WITH PREJUDICE** and, therefore, that Defendant's Rule 12(b)(1) motion to dismiss [Doc. 23] be **DENIED AS MOOT**.

All pretrial matters have been concluded with the issuance of this Report and Recommendation in accordance with 28 U.S.C. § 636(b)(1), this Court's Local Rule 72.1, and Standing Order 08-01 (N.D. Ga. June 12, 2008). The Clerk, therefore, is **DIRECTED** to terminate the reference to the Magistrate Judge.

SO RECOMMENDED THIS 5th day of February, 2013.

JANET F. KING
UNITED STATES MAGISTRATE JUDGE